ShareTech IoT 及網路行為控制可視性平台

30/100 IP 授權

ShareTech IoT 及網路行為控制可視性平台特點

1 提高網路威脅能見度

主要有三點：

1.揭露隱藏的風險

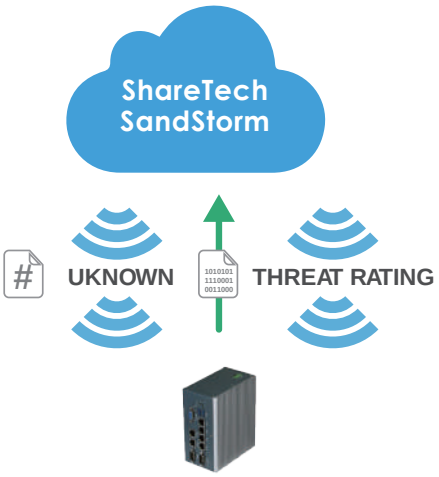
加強對高風險活動、可疑流量和進階型威脅的可見度。

2.阻止未知威脅

透過大數據分析、學習和系統漏洞補防，保護企業組織網路安全。

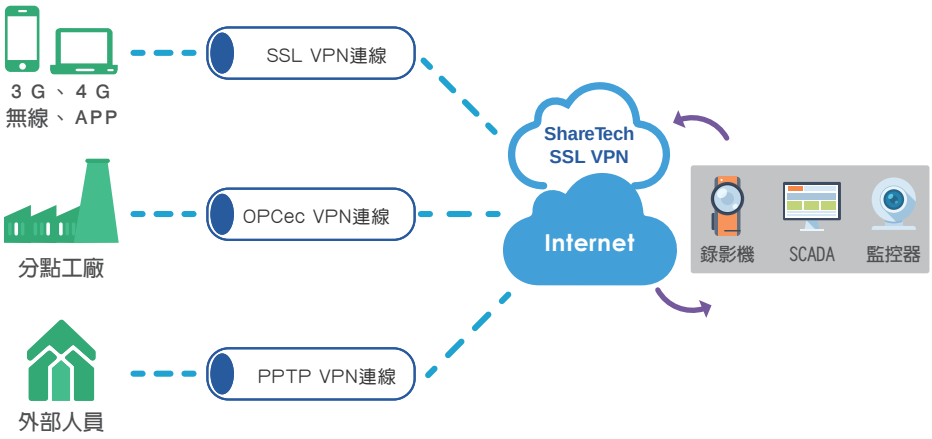
3.隔離受感染的系統

自動隔離網路中已經遭駭的系統，並阻止威脅擴散。



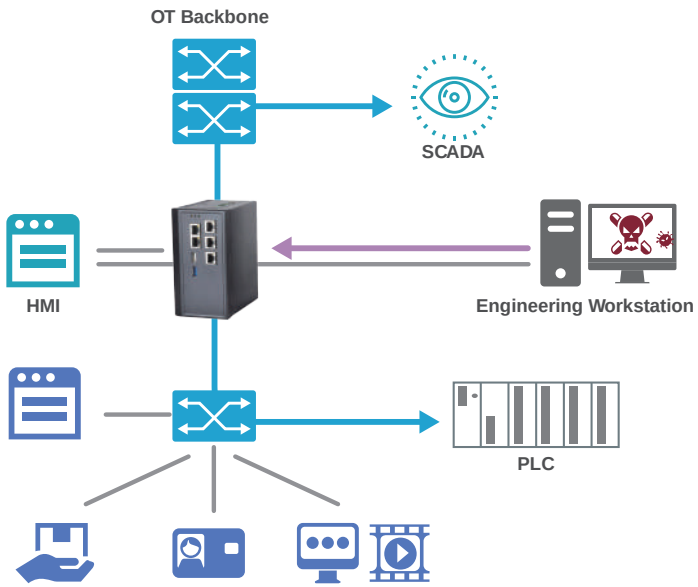
2 遠端訪問安全

開越多的對外服務Port，代表把自己暴露在外的風險因素增加，所以對於已知的連線對象，不管對方是使用動態或是固定 IP 位址，都可以利用防火牆普遍有的OPCec VPN，建立安全的VPN 通道傳遞資訊，而不需要開Port 的方式達成連線的需求。



3 多層次名單管理機制

工控機器設備每天進行的工作相當固定，與網路的運作也是全天候運作。只要設備運作正常，管理者通常不會留意設備是否有異常或是駭客滲透入侵，因此，駭客很容易藉這機會下手攻擊目標。原本在IT環境中，我們都會先開放所有網路的進出，只有針對特定的服務、程式才會進行封阻、管制。但是在OT的環境中，應該採用白名單的概念，只有列在白名單的應用程式或服務才允許被執行，才能主動做好OT設備的資安防護。



4 OPC入侵防禦機制

收集所有IT、OT網路的封包與訊號，並且採用深度封包檢測（DPI）的方式進行比對，分析通訊協定當中的每個層級，掌握出現異常數據的行為。所有異常事件都會完整記錄，透過記錄查詢可以掌握事件發生的時間、來源、目的與攻擊類型，方便管理者日後追蹤。

IPS 記錄列表

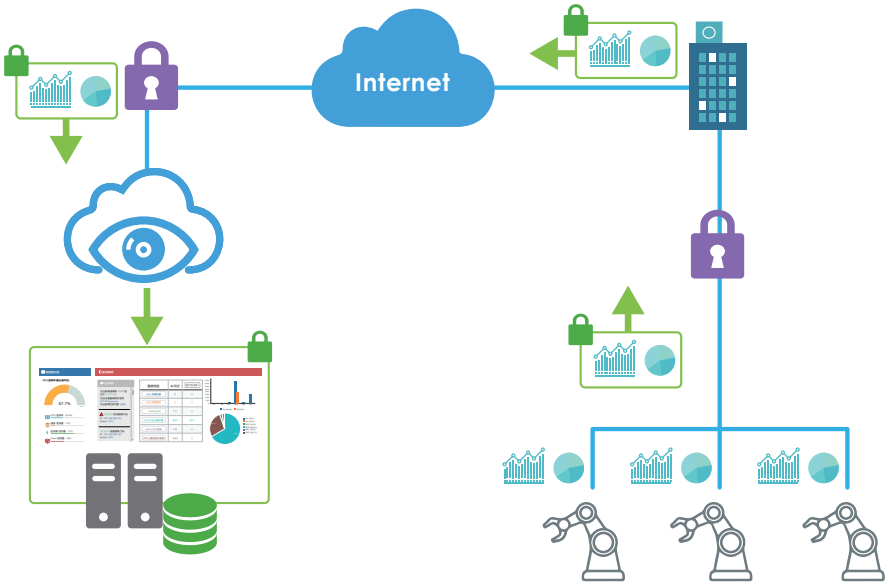
時間	分類	事件	來源 IP	目的 IP	協定	來源埠	目的埠	動作	風險程度	次數
2019-05-09 10:08:35	INFO	ET INFO Windows OS Submitting USB Metadata to Microsoft	192.168.188.102	207.46.154.155	TCP	54258	80	記錄	Low	8
2019-05-09 10:08:30	INFO	ET INFO Windows OS Submitting USB Metadata to Microsoft	192.168.188.102	207.46.154.155	TCP	54258	80	記錄	Low	14
2019-05-09 10:08:25	INFO	ET INFO Windows OS Submitting USB Metadata to Microsoft	192.168.188.102	207.46.154.155	TCP	54258	80	記錄	Low	10
2019-05-09 09:58:20	CHAT	GPL CHAT Jabber/Google Talk Outgoing Traffic	192.168.188.80	15.72.162.4	TCP	49105	5222	記錄	Low	1
2019-05-09 09:39:15	POLICY	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	192.168.188.247	185.11.254.87	TCP	43524	80	記錄	Low	1
2019-05-09 09:29:45	INFO	ET INFO Windows OS Submitting USB Metadata to Microsoft	192.168.188.81	207.46.154.155	TCP	63175	80	記錄	Low	2
2019-05-09 09:20:55	INFO	ET INFO Windows OS Submitting USB Metadata to Microsoft	192.168.188.102	207.46.155.185	TCP	54167	80	記錄	Low	10
2019-05-09 09:20:50	INFO	ET INFO Windows OS Submitting USB Metadata to Microsoft	192.168.188.102	207.46.155.185	TCP	54167	80	記錄	Low	12
2019-05-09 09:20:45	INFO	ET INFO Windows OS Submitting USB Metadata to Microsoft	192.168.188.102	207.46.155.185	TCP	54167	80	記錄	Low	4
2019-05-09 09:17:15	INFO	ET INFO Windows OS Submitting USB Metadata to Microsoft	192.168.188.102	207.46.154.155	TCP	54103	80	記錄	Low	4
2019-05-09 09:17:10	INFO	ET INFO Windows OS Submitting USB Metadata to Microsoft	192.168.188.102	207.46.154.155	TCP	54103	80	記錄	Low	12

5 Virtual Patch防護

為避免客戶重要主機遭受零時差攻擊，ShareTech OT解決方案中亦具備虛擬補丁（Virtual Patch）能力，在操作機台作業系統或軟體還未獲原廠修補更新之前，可針對性地防範漏洞的入侵。Virtual Patch，避免工廠的工控機已經沒人維護，漏洞百出，ShareTech OT安全閘道防護設備替你把關。

6 統整成威脅情報-戰情室

威脅情報-戰情室讓OT和IT管理者都能完整了解所有資料傳遞的架構，透過OT和IT的裝置數據進行收集，且會記錄所有風險類型數據，可以讓OT管理者了解廠域網路安全狀況。當有資安事件發生時，可透過詳細的風險記錄分析啟動鑑識調查。此外，提供整個OT網路的運作設備狀態能見度，顯示其IP和資產內容、顯示裝置之間使用的具體協定，並突顯潛在風險。

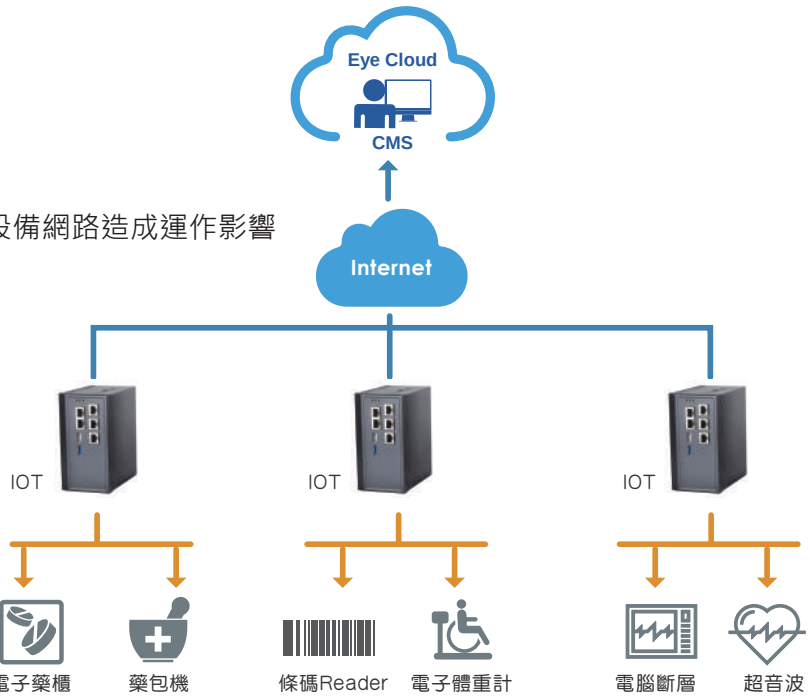


7 完整的OT網路管理平台，快速部署、簡易管理與輕鬆維護

即使最複雜的OT網路，ShareTech雲端管理平台也能讓操作管理員及網路安全專業人員，可以在單一平台，執行保護及優化OT網路的工作。

雲端管理平台與眾不同之處

- 完整呈現OT設備運作狀態
- 支援ICS設備大部份專有的通訊協定
- 即時監控與訊息通知
- 風險警告訊息通知
- 間接式連線監控管理模式，並不會對OT設備網路造成運作影響
- 設定檔備份、還原機制
- 支援設備USB設定備份機制
- 亦提供CMS服務管理功能



應用環境

1 機器/設備製造商

機器和設備製造商在面對物聯網轉型時遇到許多挑戰。它們分布於全球各地或不同位置間，但布建著許多需要連接和保護的設備。

2 智能工廠

智能工廠帶來了巨大的價值和機會，但同時也帶來了許多須特別留意的風險。從世界各地的工廠間的生產線如果提高效率和安全性，保護工廠免受內部人員，外部人員和供應商免於受到網路威脅傷害非常重要。

3 關鍵基礎設施

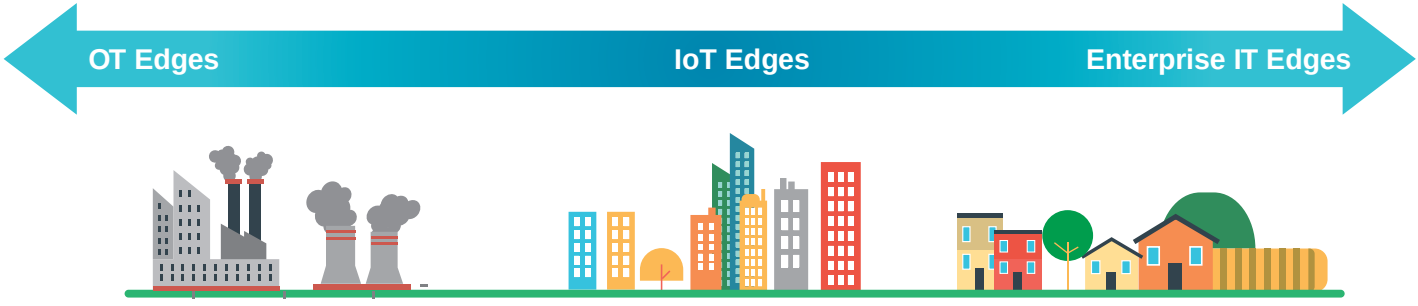
國家重要關鍵基礎設施的保護不僅可以保障經濟安全，還可以保護那些利用基礎設施的人員的實體安全。啟用遠程訪問和監視雖然可以讓管理變得更方便，但是也必須提高安全使用性。







製造廠	石油 & 天然氣	能源單位	交通運輸 & 自動化	國防 & 軍事單位	國營單位 (電信、水廠、電廠)	校園 零售分點



建構郵件安全防護系統需求

1 硬體建議需求

- CPU須為64位元，且至少為 Intel P4或更高等級系統。
- 虛擬機記憶體至少4G (含)以上。
- 硬碟至少64GB。(系統安裝基本需求)
- 支援 Intel 網卡，如使用其他廠牌網卡，請跟原廠諮詢。

2 使用者端建議需求

- 瀏覽器建議使用IE 7.0以上版本，FireFox與Google Chrome均支援。

3 環境需求

- 一條固定IP ADSL專線或PPPoE撥接線路，建議使用固定式ADSL專線，浮動IP並不適合架設。